ON THE ABSTRACT PROPERTIES OF LINEAR DEPENDENCE.[1]

By Hassler Whitney.

1. Introduction. Let $C_1, C_2, \cdots, C_n$ be the columns of a matrix $\boldsymbol{M}$. Any subset of these columns is either linearly independent or linearly dependent; the subsets thus fall into two classes. These classes are not arbitrary; for instance, the two following theorems must hold:

(a) Any subset of an independent set is independent.

(b) If $\boldsymbol{N}_p$ and $\boldsymbol{N}_{p+1}$ are independent sets of p and $p+1$ columns respectively, then $\boldsymbol{N}_p$ together with some column of $\boldsymbol{N}_{p+1}$ forms an independent set of $p+1$ columns.

There are other theorems not deducible from these; for in § 16 we give an example of a system satisfying these two theorems but not representing any matrix. Further theorems seem, however, to be quite difficult to find. Let us call a system obeying (a) and (b) a "matroid." The present paper is devoted to a study of the elementary properties of matroids. The fundamental question of completely characterizing systems which represent matrices is left unsolved. In place of the columns of a matrix we may equally well consider points or vectors in a Euclidean space, or polynomials, etc.

This paper has a close connection with a paper by the author on linear graphs;[2] we say a subgraph of a graph is independent if it contains no circuit. Although graphs are, abstractly, a very small subclass of the class of matroids, (see the appendix), many of the simpler theorems on graphs, especially on non-separable and dual graphs, apply also to matroids. For this reason, we carry over various terms in the theory of graphs to the present theory. Remarkably enough, for matroids representing matrices, dual matroids have a simple geometrical interpretation quite different from that in the case of graphs (see § 13).

The contents of the paper are as follows: In Part I, definitions of matroids in terms of the concepts rank, independence, bases, and circuits are considered, and their equivalence shown. Some common theorems are deduced (for instance Theorem 8). Non-separable and dual matroids are studied in

[1] Presented to the American Mathematical Society, September, 1934.

[2] "Non-separable and planar graphs," *Transactions of the American Mathematical Society*, vol. 34 (1932), pp. 339-362. We refer to this paper as G.

Part II; this section might replace much of the author's paper G. The subject of Part III is the relation between matroids and matrices. In the appendix, we completely solve the problem of characterizing matrices of integers modulo 2, of interest in topology.

I. Matroids.

2. Definitions in terms of rank. Let a set M of elements $e_1, e_2, \cdots, e_n$ be given. Corresponding to each subset N of these elements let there be a number $r(N)$, the *rank* of N. If the three following postulates are satisfied, we shall call this system a *matroid.*

(R_1) *The rank of the null subset is zero.*

(R_2) *For any subset N and any element e not in N,*

$$r(N+e)=r(N)+k, \qquad (k=0 \text{ or } 1).$$

(R_3) *For any subset N and elements e_1, e_2 not in N, if $r(N+e_1) = r(N+e_2)=r(N)$, then $r(N+e_1+e_2)=r(N)$.*

Evidently *any subset of a matroid is a matroid.* In what follows, M is a fixed matroid. We make the following definitions:

$$\rho(N) = \text{number of elements in } N.$$

$$n(N)=\rho(N)-r(N)=\textit{nullity} \text{ of } N.$$

N is *independent*, or, the elements of N are independent, if $n(N)=0$; otherwise, N, and its set of elements, are *dependent.*

Lemma 1. *For any N, $r(N)\geqq 0$ and $n(N)\geqq 0$. If $N\subset M$, then $r(N)\leqq r(M)$, $n(N)\leqq n(M)$.*

Lemma 2. *Any subset of an independent set is independent.*

e is *dependent on* N if $r(N+e)=r(N)$; otherwise e is *independent of* N.

A *base* is a maximal independent submatroid of M, i. e. a matroid B in M such that $n(B)=0$, while $B\subset N$, $B\neq N$ implies $n(N)>0$. See also Theorem 7. A *base complement* $A=M-B$ is the complement in M of a base B. A *circuit* is a minimal dependent matroid, i. e. a matroid P such that $n(P)>0$, while $N\subset P$, $N\neq P$ implies $n(N)=0$.[3]

Theorem 1. *N is independent if and only if it is contained in a base, or, if and only if it contains no circuit.*

[3] Compare G, Theorem 9.

THEOREM 2. *A circuit is a minimal submatroid contained in no base, i. e. containing at least one element from each base complement. A base is a maximal submatroid containing no circuit. A base complement is a minimal submatroid containing at least one element from each circuit.*

The above facts follow at once from the definitions. Note the reciprocal relationship between circuits and base complements. Note also that the definitions of independence and of being a circuit depend only on the given subset, while the property of being a base depends on the relationship of the subset to M.

3. Properties of rank. Our object here is to prove Theorem 3. The following definition will be useful:

$$\Delta(M, N) = r(M + N) - r(M). \tag{3.1}$$

LEMMA 3. $\Delta(M + e_2, e_1) \leqq \Delta(M, e_1)$.

Suppose first $r(M + e_1) = r(M) + 1$; then $r(M + e_1 + e_2) = r(M) + k$, $k = 1$ or 2. If $k = 2$, then $r(M + e_2) = r(M) + 1$, on account of (R_2), and the inequality holds; if $k = 1$, $r(M + e_2) = r(M) + l$, $l = 0$ or 1, and it holds again. If $r(M + e_2) = r(M) + 1$, the same reasoning applies. If finally $r(M + e_1) = r(M + e_2) = r(M)$, the inequality follows from (R_3).

LEMMA 4. $\Delta(M + N, e) \leqq \Delta(M, e)$.

If $N = e_1 + \cdots + e_p$, the last lemma gives

$$\Delta(M + N, e) \leqq \Delta(M + e_1 + \cdots + e_{p-1}, e) \leqq \cdots \leqq \Delta(M, e).$$

THEOREM 3. $\Delta(M + N_2, N_1) \leqq \Delta(M, N_1)$, *or,*

$$r(M + N_1 + N_2) \leqq r(M + N_1) + r(M + N_2) - r(M). \tag{3.2}$$

This is true if N_1 contains but a single element. For the general case, we apply the last lemma and induction, setting $N_1 = N' + e$:

$$\begin{aligned} \Delta(M + N_2, N_1) &= \Delta(M + N_2 + e, N') + \Delta(M + N_2, e) \\ &\leqq \Delta(M + e, N') + \Delta(M, e) = \Delta(M, N_1). \end{aligned}$$

(3.2) is evidently equivalent to:

$$r(M_1 + M_2) \leqq r(M_1) + r(M_2) - r(M_1 M_2). \tag{3.3}$$

4. Deduction of (I_1), (I_2) from (R_1), (R_2), (R_3). The first postulate

on independent sets below obviously holds if (R_1) and (R_2) hold. To prove (I_2), take N, N' as given there; then

$$r(N) = p, \qquad r(N') = p + 1.$$

We must show that for some i, $\Delta(N, e'_i) = 1$. (Then e'_i does not lie in N.) If this is not so, then on using Lemma 4 we find

$$\begin{aligned} 1 = r(N') - r(N) &\leqq \Delta(N, N') \\ &= \Delta(N, e'_1) + \Delta(N + e'_1, e'_2) + \cdots + \Delta(N + e'_1 + \cdots + e'_p, e'_{p+1}) \\ &\leqq \Delta(N, e'_1) + \Delta(N, e'_2) + \cdots + \Delta(N, e'_{p+1}) = 0, \end{aligned}$$

a contradiction.

5. Deduction of (C_1), (C_2) **from** (R_1), (R_2), (R_3). We shall need here a theorem showing how the nullity (or rank) of a matroid may be determined when we know what circuits it contains.

LEMMA 5. *Each element of a circuit is dependent on the rest of the circuit.*

If e is an element of the circuit P, then $n(P) = 1$, $n(P - e) = 0$; hence $r(P) = \rho(P) - 1 = \rho(P - e) = r(P - e)$.

LEMMA 6. *If e is dependent on P_1 but on no proper subset of P_1, then $P = P_1 + e$ is a circuit.*

As $\Delta(P_1, e) = 0$, $r(P) = r(P_1) \leqq \rho(P_1) < \rho(P)$, $n(P) > 0$, and P contains a circuit P'. If P' does not contain e, take e' in P'; then

$$\Delta(P_1 - e', e') \leqq \Delta(P' - e', e') = 0,$$

hence $r(P_1 - e') = r(P_1)$, and

$$\begin{aligned} \Delta(P_1 - e', e) &= r(P_1 - e' + e) - r(P_1 - e') \\ &\leqq r(P_1 + e) - r(P_1) = \Delta(P_1, e) = 0, \end{aligned}$$

and e is dependent on the proper subset $P_1 - e'$ of P_1, a contradiction. Therefore P' contains e. As P' is a circuit, e is dependent on the rest of P'; hence $P' = P$.

THEOREM 4. *If e is not in N, there is a circuit in $N + e$ which contains e if and only if e is dependent on N.*

Suppose $P_1 + e = P$ is a circuit, $P_1 \subset N$. Then

$$\Delta(N, e) \leqq \Delta(P_1, e) = 0,$$

and e is dependent on N. Suppose, conversely, $\Delta(N, e) = 0$. Let P_1 be a smallest subset of N on which e is dependent; then by the last lemma, $P = P_1 + e$ is a circuit. (It may be that $P = e$.)

THEOREM 5. *If N is formed element by element, then $n(N)$ is just the number of times that adding an element increases the number of circuits present.*

Say $N = e_1 + \cdot \cdot \cdot + e_p$. Then if O is the null set,

$$r(N) = \Delta(O, e_1) + \Delta(e_1, e_2) + \cdot \cdot \cdot + \Delta(e_1 + \cdot \cdot \cdot + e_{p-1}, e_p).$$

Each $\Delta(e_1 + \cdot \cdot \cdot + e_{i-1}, e_i) = 0$ or 1, and $= 0$ if and only if e_i is dependent on $e_1 + \cdot \cdot \cdot + e_{i-1}$, i. e. if and only if there is a circuit in $e_1 + \cdot \cdot \cdot + e_i$ containing e_i. The number of terms is $p = \rho(N)$, and the theorem follows.

We turn now to the proof of (C_1) and (C_2). The first is obvious. To prove the second, take P_1, P_2, e_1, e_2 as given. As

$$\Delta(P_1 - e_2, e_2) = \Delta(P_2 - e_1, e_1) = 0,$$

we have

$$\Delta(P_1 + P_2 - e_2, e_2) = \Delta(P_1 + P_2 - e_1 - e_2, e_1) = 0.$$

These equations give

$$r(P_1 + P_2 - e_1 - e_2) = r(P_1 + P_2 - e_2) = r(P_1 + P_2).$$

Using (R_2) gives

$$r(P_1 + P_2 - e_1) = r(P_1 + P_2 - e_1 - e_2);$$

hence the required circuit P_3 exists, by Theorem 4.

6. Postulates for independent sets. Let M be a set of elements. Let any subset N of M be either "independent" or "dependent." Let the two following postulates be satisfied:

(I_1) *Any subset of an independent set is independent.*

(I_2) *If $N = e_1 + \cdot \cdot \cdot + e_p$ and $N' = e'_1 + \cdot \cdot \cdot + e'_{p+1}$ are independent, then for some i such that e'_i is not in N, $N + e'_i$ is independent.*

The resulting system is equivalent to a matroid, as we now show. Given any subset N of M, we let $r(N)$ be the number of elements in a largest independent subset of N. Obviously Postulates (R_1) and (R_2) are satisfied; we must prove (R_3). Say

$$r(N+e_1)=r(N+e_2)=r(N)=r.$$

Then $r(N+e_1+e_2)=r$ or $r+1$. If it equals $r+1$, there is an independent set $N'=e'_1+\cdots+e'_{r+1}$ in $N+e_1+e_2$. Let $N''=e_1''+\cdots+e_r''$ be an independent set in N. By (I_2) there is an i such that $N''+e'_i$ is an independent set of $r+1$ elements. But $N''+e'_i$ lies in $N+e_1$ or in $N+e_2$, and hence $r(N+e_1)$ or $r(N+e_2)\geqq r+1$, a contradiction. Therefore $r(N+e_1+e_2)=r$, as required.

We have shown how to deduce either set of postulates (R) or (I) from the other. Moreover the definitions of the rank and the independence or dependence of any subset of M agree under the two systems, and hence they are equivalent.

7. Postulates for bases. Let M be a set of elements, and let each subset either be or not be a "base." We assume

(B_1) *No proper subset of a base is a base.*

(B_2) *If B and B' are bases and e is an element of B, then for some element e' in B', $B-e+e'$ is a base.*

We shall prove the equivalence of this system with the preceding one. We write here $e_1e_2\cdots$ instead of $e_1+e_2+\cdots$ for short.

THEOREM 6. *All bases contain the same number of elements.*

For suppose

$$\begin{aligned} B&=e_1\cdots e_pe_{p+1}\cdots e_qe_{q+1}\cdots e_r,\\ B'&=e_1\cdots e_pe'_{p+1}\cdots e'_q \end{aligned}$$

are bases, with exactly $e_1,\cdots,e_p$ in common, and $r>q$. We might have $p=0$. $q>p$, on account of (B_1). By (B_2), we can replace e_{p+1} in B by an element e' of B', giving a base B_1. $e'=e'_{i_1}$ is one of the elements $e'_{p+1},\cdots,e'_q$, for otherwise B_1 would be a proper subset of B. Hence

$$B_1=e_1\cdots e_pe'_{i_1}e_{p+2}\cdots e_qe_{q+1}\cdots e_r.$$

If $q>p+1$, we replace e_{p+2} in B_1 by an element e'_{i_2} of B', giving a base B_2. Continuing in this manner, we obtain finally the base

$$B_{q-p} = e_1 \cdots e_p e'_{p+1} \cdots e'_q e_{q+1} \cdots e_r.$$

But this contains B' as a proper subset, contradicting (B_1).

We shall say a subset of M is independent if it is contained in a base. (I_1) obviously holds; we shall prove (I_2). Let N, N' be independent sets in the bases B, B'. Say

$$B = e_1 \cdots e_p e_{p+1} \cdots e_q e_{q+1} \cdots e_r e_{r+1} \cdots e_s,$$
$$B' = e_1 \cdots e_p e'_{p+1} \cdots e'_q e'_{q+1} \cdots e'_r e_{r+1} \cdots e_s,$$
$$N = e_1 \cdots e_p e_{p+1} \cdots e_q, \qquad N' = e_1 \cdots e_p e'_{p+1} \cdots e'_q e'_{q+1}.$$

Then N and N' have just $e_1, \cdots, e_p$ in common, and B and B' have just these elements and $e_{r+1}, \cdots, e_s$ in common. By (B_2), there is an element e'_{i_1} of B' such that

$$B_1 = B - e_{q+1} + e'_{i_1}$$

is a base. (This element cannot be any of $e_1, \cdots, e_p, e_{r+1}, \cdots, e_s$, by (B_1).) If i_1 is one of the numbers $p+1, p+2, \cdots, q+1$, then $N + e'_{i_1}$ is in a base B_1, as required. Suppose not; then there is a base

$$B_2 = B_1 - e_{q+2} + e'_{i_2},$$

with $i_2 \neq i_1$. If $p+1 \leqq i_2 \leqq q+1$, $N + e'_{i_2}$ is in a base B_2. If not, we find a base B_3, etc. We can drop out each of the $r-q$ elements $e_{q+1}, \cdots, e_r$ in turn; as there are only $r-q-1$ elements e'_i with $i > q+1$, we find at some point a base containing $e_1, \cdots, e_q, e'_j$ with $p+1 \leqq j \leqq q+1$. Then e'_j is in N', and $N + e'_j$ is in a base and is thus independent, as required.

The definitions of base and independent sets in the two systems (I) and (B) are easily seen to agree. Suppose (I_1) and (I_2) hold. (B_1) obviously holds; using (I_2), we prove that all bases contain the same number of elements; (B_2) now follows at once from (I_2). Hence the two systems are equivalent.

Theorem 7. *B is a base in M if and only if*

$$r(B) = r(M), \qquad n(B) = 0.$$

Evidently B is a base under the given conditions. To prove the converse, we note first that there exists a base with $r(M)$ elements, as $r(M)$ is the maximum number of independent elements in M (see § 6). By Theorem 6, all bases have this many elements, and the equations follow.

Theorem 8. *If B is a base and N is independent, then for some N' in B, $N + N'$ is a base.*

This follows from repeated application of Postulate (I_2) and the last theorem.

8. Postulates for circuits. Let M be a set of elements, and let each subset either be or not be a "circuit." We assume:

(C_1) *No proper subset of a circuit is a circuit.*

(C_2) *If P_1 and P_2 are circuits, e_1 is in both P_1 and P_2, and e_2 is in P_1 but not in P_2, then there is a circuit P_3 in $P_1 + P_2$ containing e_2 but not e_1.*

(C_2) may be phrased as follows: If the circuits P_1 and P_2 have the common element e, then $P_1 + P_2 - e$ is the union of a set of circuits.

We shall define the rank of any subset of M, and shall then show that the postulates for rank are satisfied. Let $e_1, \cdots, e_p$ be any ordered set of elements of M. Set $\Gamma_i = 0$ if there is a circuit in $e_1 + \cdots + e_i$ containing e_i, and set $\Gamma_i = 1$ otherwise (compare Theorem 5). Let the "rank" of $(e_1, \cdots, e_p)$ be

$$r(e_1, \cdots, e_p) = \sum_{i=1}^{p} \Gamma_i.$$

LEMMA 7. $r(e_1, \cdots, e_{q-2}, e_{q-1}, e_q) = r(e_1, \cdots, e_{q-2}, e_q, e_{q-1})$.

To prove this, let N be the ordered set $e_1, \cdots, e_{q-2}$, and set

$$r(N) = r, \qquad r(N, e_{q-1}) = r_1, \qquad r(N, e_q) = r_2,$$
$$r(N, e_{q-1}, e_q) = r_{12}, \qquad r(N, e_q, e_{q-1}) = r_{21}.$$

CASE 1. There is no circuit in $N + e_{q-1}$ containing e_{q-1}, and none in $N + e_q$ containing e_q. Then

$$r_1 = r_2 = r + 1.$$

If there is a circuit in $N + e_{q-1} + e_q$ containing e_{q-1} and e_q, then

$$r_{12} = r_1 = r_2 = r_{21};$$

otherwise,

$$r_{12} = r_1 + 1 = r_2 + 1 = r_{21}.$$

CASE 2. There is a circuit P_2 in $N + e_{q-1}$ containing e_{q-1}, and a circuit P_1 in $N + e_{q-1} + e_q$ containing e_{q-1} and e_q. Then, by (C_2), there is a circuit P_3 in $N + e_q$ containing e_q. Hence

$$r_{12} = r_1 = r = r_2 = r_{21}.$$

CASE 3. There is a circuit P_2 as above, but no circuit P_1 as above. If there is a circuit P_3 as above, the last set of equations hold. Otherwise,

$$r_{12} = r_1 + 1 = r + 1 = r_2 = r_{21}.$$

CASE 4. There is a circuit in $N + e_q$ containing e_q. This case overlaps the two preceding ones; the proof above applies here also.

LEMMA 8. *The rank of any subset N is independent of the ordering of the elements of N.*

We saw above that interchanging the last two elements of any subset does not alter the rank; hence, evidently, interchanging any two adjacent elements leaves the rank unchanged. Any ordering of M may be obtained from any other by a number of interchanges of adjacent elements; the rank remains unchanged at each step, proving the lemma.

Postulates (R_1) and (R_2) are obviously satisfied. To prove (R_3), suppose $r(N + e_1) = r(N + e_2) = r(N)$. Then there is a circuit in $N + e_1$ containing e_1 and one in $N + e_2$ containing e_2; hence $r(N + e_1 + e_2) = r(N)$.

The definitions of rank and of circuits under the two systems (R), (C) agree, and hence the systems are equivalent.

9. Fundamental sets of circuits. The circuits $P_1, \cdots, P_q$ of a matroid M form a *fundamental set of circuits* if $q = n(M)$ and the elements $e_1, \cdots, e_n$ of M can be ordered so that P_i contains e_{n-q+i} but no e_{n-q+j} $(j > i)$. The set is *strict* if P_i contains e_{n-q+i} but no e_{n-q+j} $(0 < j < i$ or $j > i)$. These sets may be called sets *with respect to* $e_{n-q+1}, \cdots, e_n$.

THEOREM 9. *If $B = e_1 + \cdots + e_{n-q}$ is a base in $M = e_1 + \cdots + e_n$, then there is a strict fundamental set of circuits with respect to $e_{n-q+1}, \cdots, e_n$; these circuits are uniquely determined.*

As $r(B) = r(M)$, $\Delta(B, e_i) = 0$ $(i = n - q + 1, \cdots, n)$. Hence, by Theorem 4, there is a circuit P_i containing e_i and elements (possibly) of B. $P_{n-q+1}, \cdots, P_n$ is the required set. Suppose, for a given i, there were also a circuit $P'_i \neq P_i$. Then Postulate (C_2) applied to P_i and P'_i would give us a circuit P in B, which is impossible.

This theorem corresponds to the theorem that if a square submatrix N of a matrix M is non-singular, then N can be turned into the unit matrix by a linear transformation on the rows of M.

THEOREM 10. *If $P_1, \cdots, P_q$ form a fundamental set of circuits with*

respect to $e_{n-q+1},\cdots,e_n$, *then there is a unique strict set* $P'_1,\cdots,P'_q$ *with respect to* $e_{n-q+1},\cdots,e_n$.

Set $B=M-(e_{n-q+1}+\cdots+e_n)$. The existence of $P_1,\cdots,P_q$ shows that $r(M)=r(M-e_n)=\cdots=r(B)$. Hence $\rho(B)=n-q=r(M)=r(B)$, and B is a base, by Theorem 7. Theorem 9 now applies.

Note that a matroid is not uniquely determined by a fundamental set of circuits (but see the appendix). This is shown by the following two matroids, in each of which the first two circuits form a strict fundamental set:

M, with circuits 1234, 1256, 3456;
M', with circuits 1234, 1256, 13456, 23456.

II. Separability, Dual Matroids.

10. Separable matroids. If $M=M_1+M_2$, then $r(M)\leqq r(M_1)+r(M_2)$, on account of (3.3). If it is possible to divide the elements of M into two groups, M_1 and M_2, each containing at least one element, such that

$$r(M)=r(M_1)+r(M_2), \tag{10.1}$$

or, which is equivalent (as M_1 and M_2 have no common elements),

$$n(M)=n(M_1)+n(M_2), \tag{10.2}$$

we shall say M is *separable*; otherwise, M is *non-separable*.[4] Any single element forms a non-separable matroid. Any maximal non-separable part of M is a *component* of M.[5]

Theorem 11. *If*

$$M=M_1+M_2, \qquad r(M)=r(M_1)+r(M_2),$$
$$M'_1\subset M_1, \qquad M'_2\subset M_2, \qquad M'=M'_1+M'_2,$$

then

$$r(M')=r(M'_1)+r(M'_2).$$

Set $M_1''=M_1-M_1'$, $M_2''=M_2-M_2'$. The relations (see Theorem 3)

$$\begin{aligned} r(M) &= \Delta(M_1+M_2',M_2'')+\Delta(M',M_1'')+r(M') \\ &\leqq \Delta(M_2',M_2'')+\Delta(M_1',M_1'')+r(M') \\ &= r(M_2)-r(M_2')+r(M_1)-r(M_1')+r(M') \end{aligned}$$

[4] Compare G, Theorem 15.
[5] See G, § 4.

together with the fact that $r(M) = r(M_1) + r(M_2)$ show that $r(M') \geqq r(M'_1) + r(M'_2)$ and hence $r(M') = r(M'_1) + r(M'_2)$.

THEOREM 12.[6] *If $M = M_1 + M_2$, $r(M) = r(M_1) + r(M_2)$, M' is non-separable, and $M' \subset M$, then either $M' \subset M_1$ or $M' \subset M_2$.*

For suppose $M' = M'_1 + M'_2$, $M'_1 \subset M_1$, $M'_2 \subset M_2$, and M'_1 and M'_2 each contain an element. By the last theorem, $r(M') = r(M'_1) + r(M'_2)$, which cannot be.

THEOREM 13. *If M_1 and M_2 are non-separable matroids with a common element e, then $M = M_1 + M_2$ is non-separable.*

For suppose $M = M'_1 + M'_2$, $r(M) = r(M'_1) + r(M'_2)$. By the last theorem, $M_1 \subset M'_1$ or $M_1 \subset M'_2$, and $M_2 \subset M'_1$ or $M_2 \subset M'_1$; this shows that either M'_1 or M'_2 is void.

THEOREM 14. *No two distinct components of M have common elements.*

This is a consequence of the last theorem. From this follows:

THEOREM 15.[7] *Any matroid may be expressed as a sum of components in a unique manner.*

THEOREM 16.[8] *A non-separable matroid M of nullity 1 is a circuit, and conversely.*

If M_1 is a proper non-null subset of the non-separable matroid M, and $M_2 = M - M_1$, then $r(M) < r(M_1) + r(M_2)$. Hence

$$1 = n(M) > n(M_1) + n(M_2),$$

and $n(M_1) = 0$, proving that M is a circuit.

Conversely, if $M = M_1 + M_2$ is a circuit, and M_1 and M_2 each contain elements, then

$$\begin{aligned} r(M_1) + r(M_2) &= \rho(M_1) + \rho(M_2) - n(M_1) - n(M_2) \\ &= \rho(M) > r(M), \end{aligned}$$

showing that M is non-separable.

[6] Compare G, Lemma, p. 344.
[7] Compare G, Theorem 12.
[8] Compare G, Theorem 10.

Lemma 9. *Let $M = M_1 + M_2$ be non-separable, and let M_1 and M_2 each contain elements but have no common elements. Then there is a circuit P in M containing elements of both M_1 and M_2.*

Suppose there were no such circuit. Say $M_2 = e_1 + \cdots + e_s$. Using Theorem 4, we see that

$$\Delta(M_1 + e_1 + \cdots + e_{i-1}, e_i) = \Delta(e_1 + \cdots + e_{i-1}, e_i) \quad (i = 1, \cdots, s),$$

and hence $r(M) = r(M_1) + r(M_2)$, a contradiction.

Theorem 17.[9] *Any non-separable matroid M of nullity $n > 0$ can be built up in the following manner: Take a circuit M_1; add a set of elements which forms a circuit with one or more elements of M_1, forming a non-separable matroid M_2 of nullity 2 (if $n(M) > 1$); repeat this process till we have $M_n = M$.*

As $n > 0$, M contains a circuit M_1. If $n > 1$, we use the preceding lemma $n - 1$ times. The matroid at each step is non-separable, by Theorems 16 and 13.

Theorem 18.[10] *Let $M = M_1 + \cdots + M_p$, and let $M_1, \cdots, M_p$ be non-separable. Then the following statements are equivalent:*

(1) *$M_1, \cdots, M_p$ are the components of M.*

(2) *No two of the matroids $M_1, \cdots, M_p$ have common elements, and there is no circuit in M containing elements of more than one of them.*

(3) $r(M) = r(M_1) + \cdots + r(M_p)$.

We cannot replace rank by nullity in (3); see G, p. 347.

(2) follows from (1) on application of Theorems 13 and 16.

To prove (1) from (2), take any M_i. If it is not a component of M, there is a larger non-separable submatroid M'_i of M containing it. By Lemma 9, there is a circuit P in M'_i containing elements of M_i and elements not in M_i; P must contain elements of some other M_j, a contradiction.

Next we prove (3) from (1). If $p > 1$, M is separable; say $M = M'_1 + M'_2$, $r(M) = r(M'_1) + r(M'_2)$. By Theorem 12, each M_i is in either M'_1 or M'_2; hence M'_1 and M'_2 are each a sum of components of M. If one of these

[9] See G, Theorem 19; also Whitney, "2-isomorphic graphs," *American Journal of Mathematics*, vol. 55 (1933), p. 247, footnote.

[10] Compare G, Theorem 17.

contains more than one component, we separate it similarly, etc. (3) now follows easily.

Finally we prove (1) from (3). Let M' be a component of M, and suppose it has an element in M_i. As

$$r(M) = r(M_i) + \sum_{j \neq i} r(M_j),$$

M' is contained in M_i, by Theorem 12; as M_i is non-separable, $M' = M_i$.

THEOREM 19.[11] *The elements e_1 and e_2 are in the same component of M if and only if they are contained in a circuit P.*

If e_1 and e_2 are both in P, they are part of a non-separable matroid, which lies in a single component of M. Suppose now e_1 and e_2 are in the same component M_0 of M, and suppose there is no circuit containing them both. Let M_1 be e_1 plus all elements which are contained in a circuit containing e_1. By Lemma 9, there is a subset M^* of $M_0 - M_1$ which forms with part of M_1 a circuit P_3. P_3 does not contain e_1. If e'_4 is an element of P_3 in M_1, there is a circuit P_1 in M_1 containing e_1 and e'_4. Let e_3 be an element of M^*. Then in $M_1 + M^*$ there are circuits P_1 and P_3 which contain e_1 and e_3 respectively, and have a common element.

Let M' be a smallest subset of M_0 which contains circuits P'_1 and P'_3 such that one contains e_1, the other contains e_3, and they have common elements. Then P'_1 and P'_3 are distinct, and $M' = P'_1 + P'_3$. Let e_4 be a common element. By Postulate (C_2), there is a circuit P_1 in $M' - e_4$ containing e_1, and a circuit P_3 in $M' - e_4$ containing e_3. By the definition of M', P_1 and P_3 have no common elements. By Postulate (C_1), P_1 is not contained in P'_1; hence it contains an element e_5 of $M' - P'_1$. P_3 does not contain e_5. As P_3 is not contained in P'_3, it contains an element e_6 of P'_1. But now P'_1 contains e_1, P_3 contains e_3, $P'_1 + P_3$ have a common element e_6, and $P'_1 + P_3$ does not contain e_5 and is thus a proper subset of M', a contradiction. This proves the theorem.

11. Dual matroids. Suppose there is a $1-1$ correspondence between the elements of the matroids M and M', such that if N is any submatroid of M and N' is the complement of the corresponding matroid of M', then

$$r(N') = r(M') - n(N). \tag{11.1}$$

[11] Compare D. König, *Acta Litterarum ac Scientiarum Szeged*, vol. 6, pp. 155-179, 4. (p. 159). The present theorem shows that a "glied" is the same as a component.

We say then that M' is a *dual* of M.[12]

THEOREM 20. *If M' is a dual of M, then*

$$r(M') = n(M), \qquad n(M') = r(M).$$

Set $N = M$; then $n(N) = n(M)$. In this case N' is the null matroid, and $r(N') = 0$. (11.1) now gives $r(M') = n(M)$. Also

$$n(M') = \rho(M') - r(M') = \rho(M) - n(M) = r(M).$$

THEOREM 21. *If M' is a dual of M, then M is a dual of M'.*

Take any N and corresponding N' as before. The equations

$$r(N') = r(M') - n(N), \qquad r(M') = n(M),$$
$$\rho(N) + \rho(N') = \rho(M)$$

give

$$\begin{aligned} r(N) &= \rho(N) - n(N) = \rho(N) - [r(M') - r(N')] \\ &= \rho(N) - n(M) + [\rho(N') - n(N')] \\ &= \rho(M) - n(M) - n(N') = r(M) - n(N'), \end{aligned}$$

as required.

THEOREM 22. *Every matroid has a dual.*

This is in marked contrast to the case of graphs, for only a planar graph has a dual graph (see G, Theorem 29).

Let M' be a set of elements in $1 —$ correspondence with elements of M. If N' is any subset of M', let N be the complement of the corresponding subset of M, and set $r(N') = n(M) - n(N)$. (R_1), (R_2), (R_3) are easily seen to hold in M', as they hold in M; hence M' is a matroid. Obviously $r(M') = n(M)$, and M' is a dual of M.

THEOREM 23. *M and M' are duals if and only if there is a $1 - 1$ correspondence between their elements such that bases in one correspond to base complements in the other.*

Suppose first M and M' are duals. Let B be a base in either matroid, say in M, and let B' be the complement of the corresponding submatroid of the other matroid, M'. Then

---

[12] Compare G, § 8. Theorems 20, 21, 24, 25 correspond to Theorems 20, 21, 23, 25 in G. Note that *two duals of the same matroid are isomorphic,* that is, there is a $1 - 1$ correspondence between their elements such that corresponding subsets have the same rank. Such a statement cannot be made about graphs. Compare H. Whitney, "2-isomorphic graphs," *American Journal of Mathematics,* vol. 55 (1933), pp. 245-254.

$$r(B') = r(M') - n(B) = r(M'),$$
$$n(B') = r(M) - r(B) = 0,$$

and B' is a base in M', by Theorem 7.

Suppose, conversely, that bases in one correspond to base complements in the other. Let N be a submatroid of M and let N' be the complement of the corresponding submatroid of M'. There is a base B' in M' with $r(N')$ elements in N', by Theorem 8. The complement in M of the submatroid corresponding to B' in M' is a base B in M with $\rho(N') - r(N') = n(N')$ elements in $M - N$, and hence with $r(M) - n(N')$ elements in N. This shows that

$$r(N) = r(M) - n(N') + k, \qquad k \geqq 0.$$

In a similar fashion we see that

$$r(N') = r(M') - n(N) + k', \qquad k' \geqq 0.$$

As B contains $r(M)$ elements and B' contains $r(M')$ elements, $r(M) + r(M') = \rho(M)$. Hence, adding the above equations,

$$\begin{aligned} k + k' &= r(N) + r(N') + n(N) + n(N') - r(M) - r(M') \\ &= \rho(N) + \rho(N') - \rho(M) = 0. \end{aligned}$$

Hence $k = 0$, and the first equation above shows that M and M' are duals.

There are various other ways of stating conditions on certain submatroids of M and M' which will ensure these matroids being duals.[13]

THEOREM 24. *Let $M_1, \cdots, M_p$ and $M'_1, \cdots, M'_p$ be the components of M and M' respectively, and let M'_i be a dual of M_i $(i = 1, \cdots, p)$. Then M' is a dual of M.*

Let N be any submatroid of M, and let the parts of N in $M_1, \cdots, M_p$ be $N_1, \cdots, N_p$. Let N'_i be the complement in M'_i of the submatroid corresponding to N_i; then $N' = N'_i + \cdots + N'_p$ is the complement in M' of the submatroid corresponding to N. By Theorems 18 and 11 we have

$$r(N') = r(N'_1) + \cdots + r(N'_p), \qquad n(N) = n(N_1) + \cdots + n(N_p).$$

Also

$$r(M') = r(M'_1) + \cdots + r(M'_p), \qquad r(N'_i) = r(M'_i) - n(N_i);$$

adding the last set of equations gives $r(N') = r(M') - n(N)$, as required.

---

[13] See for instance a paper by the author "Planar graphs," *Fundamenta Mathematicae*, vol. 21 (1933), pp. 73-84, Theorem 2. Cut sets may of course be defined in terms of rank.

THEOREM 25. *Let M and M' be duals, and let $M_1, \cdots, M_p$ be the components of M. Let $M'_1, \cdots, M'_p$ be the corresponding submatroids of M'. Then $M'_1, \cdots, M'_p$ are the components of M', and M'_i is a dual of M_i $(i = 1, \cdots, p)$.*

The complement in M of the submatroid corresponding to M'_i in M' is $\sum_{j \neq i} M_j$. Hence, as M and M' are duals and the M_j $(j \neq i)$ are the components of $\sum_{j \neq i} M_j$ (see Theorem 18),

$$r(M'_i) = r(M') - n(\sum_{j \neq i} M_j) = r(M') - \sum_{j \neq i} n(M_j).$$

Adding gives

$$\sum_i r(M'_i) = pr(M') - (p-1) \sum_j n(M_j) = pr(M') - (p-1) n(M)$$
$$= pr(M') - (p-1) r(M') = r(M').$$

Therefore, by Theorem 12, each component of M' is contained in some M'_i. In the same way we see that each component of M is contained in a matroid corresponding to a component of M'; hence the components of one matroid correspond exactly to the components of the other.

Let N_i be any submatroid of M_i, and let N' and N'_i be the complements in M' and M'_i of the submatroid corresponding to N_i. The equations

$$r(M') = \sum_j r(M'_j), \qquad r(N') = r(N'_i) + \sum_{j \neq i} r(M'_j),$$
$$r(N') = r(M') - n(N_i),$$

give

$$r(N'_i) = r(M'_i) - n(N_i),$$

which shows that M'_i is a dual of M_i.

THEOREM 26. *A dual of a non-separable matroid is non-separable.*

This is a consequence of the last theorem.

III. MATRICES AND MATROIDS.

12. Matrices, matroids, and hyperplanes. Consider the matrix

$$\boldsymbol{M} = \left\| \begin{matrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{m1} & \cdots & a_{mn} \end{matrix} \right\|;$$

let its columns be $C_1, \cdots, C_n$. Any subset $\boldsymbol{N}$ of these columns forms a matrix, and this matrix has a rank, $r(\boldsymbol{N})$. If we consider the columns as abstract elements, we have a matroid M. The proof of this is simple if we consider the rank of a matrix as the number of linearly independent columns in it. (R_1) and (R_2) are then obvious. To prove (R_3), suppose $r(\boldsymbol{N} + C_1) = r(\boldsymbol{N} + C_2) = r(\boldsymbol{N})$; then C_1 and C_2 can each be expressed as a linear combination of the other columns of $\boldsymbol{N}$, and hence $r(\boldsymbol{N} + C_1 + C_2) = r(\boldsymbol{N})$. The terms independent and base carry over to matrices and agree with the ordinary definitions; a base in $\boldsymbol{M}$ is a minimal set of columns in terms of which all remaining columns of $\boldsymbol{M}$ may be expressed.

We may interpret $\boldsymbol{M}$ geometrically in two different ways; the second is the more interesting for our purposes:

(a) Let E_m be Euclidean space of m dimensions. Corresponding to each column C_i of $\boldsymbol{M}$ there is a point X_i in E_m with coördinates $a_{1i}, \cdots, a_{mi}$. The subset $C_{i_1}, \cdots, C_{i_p}$ of $\boldsymbol{M}$ is linearly independent if and only if the points $O = (0, \cdots, 0)$, $X_{i_1}, \cdots, X_{i_p}$ are linearly independent in E_m, i. e. if and only if these $p + 1$ points determine a hyperplane in E_m of dimension p. A base in $\boldsymbol{M}$ corresponds to a minimal set of points $X_{i_1}, \cdots, X_{i_p}$ in E_m such that each X_j of $\boldsymbol{M}$ lies in the hyperplane determined by $O, X_{i_1}, \cdots, X_{i_p}$. Then p is the rank of $\boldsymbol{M}$.

(b) Let E_n be Euclidean space of n dimensions. Let $R_1, \cdots, R_m$ be the rows of $\boldsymbol{M}$. If $Y_1, \cdots, Y_m$ are the corresponding points of E_n: $Y_i = (a_{i1}, \cdots, a_{in})$, then the points $O, Y_1, \cdots, Y_m$ determine a hyperplane $H = H(\boldsymbol{M})$, which we shall call the *hyperplane associated with* $\boldsymbol{M}$. The dimension $d(H)$ of H is $r(\boldsymbol{M})$. Let $\boldsymbol{N} = C_{i_1} + \cdots + C_{i_p}$ be a subset of $\boldsymbol{M}$, and let E' be the p-dimensional coördinate subspace of E_n containing the x_{i_1} and ... and the x_{i_p} axes. The j-th row of $\boldsymbol{N}$ corresponds to the point Y'_j in E' with coördinates $(a_{j i_1}, \cdots, a_{j i_p})$; this is just the projection of Y_j onto E'. If H' is the hyperplane in E' determined by the points $O, Y'_1, \cdots, Y'_m$, then H' is exactly the projection of H onto E', and

$$d(H') = r(\boldsymbol{N}). \tag{12.1}$$

Let $\boldsymbol{N} = (C_{i_1}, \cdots, C_{i_p})$ be any subset of $\boldsymbol{M}$, and let E', H' correspond to $\boldsymbol{N}$. Then $\boldsymbol{N}$ *is independent if and only if*

$$d(H') = p,$$

and is a base if and only if

$$d(H') = d(H) = p.$$

THEOREM 27. *There is a unique matroid M associated with any hyperplane H through the origin in E_n.*

Let M contain the elements $e_1, \cdots, e_n$, one corresponding to each coördinate of E_n. Given any subset $e_{i_1}, \cdots, e_{i_p}$, we let its rank be the dimension of the projection of H onto the corresponding coördinate hyperplane E' of E_n. It was seen above that if $\boldsymbol{M}$ is any matrix determining H, then M is the matroid associated with $\boldsymbol{M}$.

13. Orthogonal hyperplanes and dual matroids. We prove the following theorem:

THEOREM 28. *Let H be a hyperplane through the origin in E_n, of dimension r, and let H' be the orthogonal hyperplane through the origin, of dimension $n-r$. Let M and M' be the associated matroids. Then M and M' are duals.*

We shall show that bases in one matroid correspond to base complements in the other; Theorem 23 then applies. Let

$$\boldsymbol{M} = \left\| \begin{matrix} a_{11} \cdots a_{1n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1} \cdots a_{rn} \end{matrix} \right\|, \qquad \boldsymbol{M}' = \left\| \begin{matrix} b_{11} \quad \cdots b_{1n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ b_{n-r,1} \cdots b_{n-r,n} \end{matrix} \right\|$$

be matrices determining H and H' respectively. Say the first r columns of $\boldsymbol{M}$ form a base in $\boldsymbol{M}$, i. e. the corresponding determinant A is $\neq 0$. As H and H' are orthogonal, we have for each i and j

$$a_{i1}b_{j1} + a_{i2}b_{j2} + \cdots + a_{in}b_{jn} = 0.$$

Keeping j fixed, we have a set of r linear equations in the b_{jk}. Transpose the last $n-r$ terms in each equation to the other side, and solve for b_{jk}. We find

$$b_{jk} = \frac{-1}{A} \sum_{l=r+1}^{n} b_{jl} \left| \begin{matrix} a_{11} \cdots a_{1l} \cdots a_{1r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1} \cdots a_{rl} \cdots a_{rr} \end{matrix} \right| = \sum_{l=r+1}^{n} c_{kl} b_{jl} \qquad (k = 1, \cdots, r).$$

This is true for each $j = 1, \cdots, n-r$, and the c_{kl} are independent of j. Thus the k-th column of $\boldsymbol{M}'$ is expressed in terms of the last $n-r$ columns. As this is true for $k = 1, \cdots, r$, the last $n-r$ columns form a base in $\boldsymbol{M}'$, as required.

14. The circuit matrix of a given matrix. Consider the matrix $\boldsymbol{M}$ of § 12. Suppose the columns $C_{i_1}, \cdots, C_{i_p}$ form a circuit, i. e. the corresponding

elements of the corresponding matroid form a circuit. Then these columns are linearly dependent, and there are numbers $b_1, \cdots, b_n$ such that

$$
\begin{array}{llr}
(14.1) & a_{i1}b_1 + \cdots + a_{in}b_n = 0 & (i = 1, \cdots, m), \\
& b_j = 0 \quad (j \neq i_1, \cdots, i_p), & b_j \neq 0 \quad (j = i_1, \cdots, i_p).
\end{array}
$$

The b_j are all $\neq 0$ $(j = i_1, \cdots, i_p)$, for otherwise a proper subset of the columns would be dependent, contrary to the definition of a circuit. (They are uniquely determined except for a constant factor; see Lemma 11.) Suppose the circuits of $\boldsymbol{M}$ are $P_1, \cdots, P_s$. Then there are corresponding sets of numbers $b_{i1}, \cdots, b_{in}$ $(i = 1, \cdots, s)$, forming a matrix

$$
\boldsymbol{M}' = \left\| \begin{matrix} b_{11} \cdots b_{1n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ b_{s1} \cdots b_{sn} \end{matrix} \right\|,
$$

the *circuit matrix* of the matrix $\boldsymbol{M}$.

THEOREM 29. *Let $P_1, \cdots, P_q$ be a fundamental set of circuits in $\boldsymbol{M}$* (see § 9). *Then the corresponding rows of the circuit matrix $\boldsymbol{M}'$ form a base for the rows of $\boldsymbol{M}'$. Hence $r(\boldsymbol{M}') = q = n(\boldsymbol{M})$.*

Suppose the columns of $\boldsymbol{M}$ are ordered so that P_i contains C_{n-q+i} but no column C_{n-q+j} $(j > i)$. Then if the corresponding row of $\boldsymbol{M}'$ is $R'_i = (b_{i1}, \cdots, b_{in})$, we have $b_{i,n-q+i} \neq 0$ and $b_{i,n-q+j} = 0$ $(j > i)$. Hence the rows $R'_1, \cdots, R'_q$ of $\boldsymbol{M}'$ are linearly independent, and $r(\boldsymbol{M}') \geqq q$. Hence $r(\boldsymbol{M}') = n(\boldsymbol{M}) = q$, and each row of $\boldsymbol{M}'$ may be expressed in terms of $R'_1, \cdots, R'_q$.

THEOREM 30. *If $\boldsymbol{M}'$ is the circuit matrix of $\boldsymbol{M}$ and H', H are the corresponding hyperplanes, then H' is the hyperplane of maximum dimension orthogonal to H.*

This is a consequence of (14.1) and the last theorem.

THEOREM 31. *The matroids corresponding to a matrix and its circuit matrix are duals.*

This follows from the last theorem and Theorem 28.

15. On the structure of a circuit matrix. Let M be any matroid, and M', its dual. If there exists a matrix $\boldsymbol{M}$ corresponding to M, it is perhaps most easily constructed by considering it as the circuit matrix of a matrix $\boldsymbol{M}'$

corresponding to M'. Let H and H' be the hyperplanes corresponding to $\boldsymbol{M}$ and $\boldsymbol{M}'$. We shall say the set of numbers $(a_1, \cdots, a_n)$ is in $Z_{i_1 \cdots i_p}$ if

$$a_j \neq 0 \quad (j = i_1, \cdots, i_p), \qquad a_j = 0 \quad (j \neq i_1, \cdots, i_p).$$

If $(a_1, \cdots, a_n)$ is in H and in $Z_{i_1 \cdots i_p}$, then the columns $C_{i_1}, \cdots, C_{i_p}$ of $\boldsymbol{M}'$ are dependent, evidently.

LEMMA 10. *Let $(b_1, \cdots, b_n)$ be a point of H. If it is in $Z_{i_1 \cdots i_p}$, then the matroid $N' = e_{i_1} + \cdots + e_{i_p}$ is the union of a set of circuits in M'.*

Here e_i in M' corresponds to C_i in $\boldsymbol{M}$. We need merely show that for each i_s there is a circuit P in N' containing e_{i_s}. Let $k_1 = i_s, k_2, \cdots, k_q$ be a minimal set of numbers from $(i_1, \cdots, i_p)$ containing i_s such that there is a point $(c_1, \cdots, c_n)$ of H in $Z_{k_1 \cdots k_q}$; then $e_{k_1} + \cdots + e_{k_q}$ is the required circuit. For if it were not a circuit, there would be a proper subset $(l_1, \cdots, l_r)$ of $(k_1, \cdots, k_q)$ and a point $(d_1, \cdots, d_n)$ of H in $Z_{l_1 \cdots l_r}$. No $l_i = k_1$, on account of the minimal property of $(k_1, \cdots, k_q)$. Say $l_1 = k_t$, and set

$$a_i = d_{k_t} c_i - c_{k_t} d_i \qquad (i = 1, \cdots, n).$$

Then $(a_1, \cdots, a_n)$ is in H and in $Z_{m_1 \cdots m_u}$ with $(m_1, \cdots, m_u)$ a proper subset of $(k_1, \cdots, k_q)$ containing k_1, again a contradiction.

LEMMA 11. *If $P = e_{i_1} + \cdots + e_{i_p}$ is a circuit of M' and $(b_1, \cdots, b_n)$ and $(b'_1, \cdots, b'_n)$ are in H and in $Z_{i_1 \cdots i_p}$, then these two sets are proportional.*

For otherwise, $(c_1, \cdots, c_n)$ with $c_i = b'_{i_1} b_i - b_{i_1} b'_i$ would be a point of H in some $Z_{k_1 \cdots k_q}$ with $(k_1, \cdots, k_q)$ a proper subset of $(i_1, \cdots, i_p)$, and P would not be a circuit.

It is instructive to show directly that Postulate (C_2) holds for matrices: P_1 and P_2 are represented by rows $(b_1, \cdots, b_n)$ and $(b'_1, \cdots, b'_n)$ of $\boldsymbol{M}$, lying in $Z_{12 i_1 \cdots i_p}$ and $Z_{1 k_1 \cdots k_q}$ respectively, where $k_1, \cdots, k_q \neq 2$. Set $c_i = b'_1 b_i - b_1 b'_i$; then $(c_1, \cdots, c_n)$ is in H and in $Z_{2 l_1 \cdots l_r}$, with $(l_1, \cdots, l_r)$ a subset of $(i_1, \cdots, i_p, k_1, \cdots, k_q)$; the existence of P_3 now follows from Lemma 10.

THEOREM 32. *Let $\boldsymbol{M}$ be the circuit matrix of $\boldsymbol{M}'$. Let $P_1, \cdots, P_q$ form a strict fundamental set of circuits in M' with respect to $e_{n-q+1}, \cdots, e_n$, and let the first q rows in $\boldsymbol{M}$ correspond to $P_1, \cdots, P_q$. Let $(i_1, \cdots, i_s)$ be any set of numbers from $(1, \cdots, q)$, let $(j_1, \cdots, j_s)$ be any set from $(1, \cdots, n-q)$, and let $(i'_1, \cdots, i'_{q-s})$ be the set complementary to $(i_1, \cdots, i_s)$ in $(1, \cdots, q)$.*

Then the determinant D in $\boldsymbol{M}$ with rows $i_1, \cdots, i_s$ and columns $j_1, \cdots, j_s$ equals zero if and only if the determinant D' with rows $1, \cdots, q$ and columns $j_1, \cdots, j_s$, $n - q + i'_1, \cdots, n - q + i'_{q-s}$ equals zero, or, if and only if there exists a circuit P in $\boldsymbol{M}'$ containing none of the columns $e_{j_1}, \cdots, e_{j_s}$, $e_{n-q+i'_1}, \cdots, e_{n-q+i'_{q-s}}$.

In the matrix of the last $q = r(\boldsymbol{M})$ columns of $\boldsymbol{M}$, the terms along the main diagonal and only those are $\neq 0$. If we expand D' by Laplace's expansion in terms of the columns $n - q + i'_1, \cdots, n - q + i'_{q-s}$, we see at once that $D' = 0$ if and only if $D = 0$.

Suppose $D = 0$. Then there is a set of numbers $(\alpha_1, \cdots, \alpha_q)$, not all zero, with $\alpha_i = 0$ $(i \neq i_1, \cdots, i_s)$, such that

$$b_k = \alpha_1 b_{1k} + \cdots + \alpha_q b_{qk} = 0 \qquad (k = j_1, \cdots, j_s),$$

$(b_{i1}, \cdots, b_{in})$ being the i-th row of $\boldsymbol{M}$., $b_k = 0$ also for $k = n - q + i'_1, \cdots,$ $n - q + i'_{q-s}$, as each term is zero for such k. The point $(b_1, \cdots, b_n)$ is in H. Any circuit given by Lemma 10 is the required circuit P.

Suppose the circuit P exists. Then it is represented by a row $(b_1, \cdots, b_n)$ in $\boldsymbol{M}$. As the first q rows of $\boldsymbol{M}$ are of rank $q = r(\boldsymbol{M})$, $(b_1, \cdots, b_n)$ can be expressed in terms of them; say $b_k = \Sigma \alpha_i b_{ik}$. As $b_k = 0$ $(k = n - q + i'_1, \cdots,$ $n - q + i'_{q-s})$, certainly $\alpha_k = 0$ $(k = i'_1, \cdots, i'_{q-s})$. $D = 0$ now follows from the fact that $b_k = 0$ $(k = j_1, \cdots, j_s)$.

16. A matroid with no corresponding matrix.[14] The matroid M' has seven elements, which we name $1, \cdots, 7$. The bases consist of all sets of three elements except

(16.1) 124, 135, 167, 236, 257, 347, 456.

Defining rank in terms of bases, we have: Each set of k elements is of rank k if $k \leqq 2$ and of rank 3 if $k \geqq 4$; a set of three elements is of rank 2 if the set is in (16.1) and is of rank 3 otherwise. It is easy to see that the postulates for rank are satisfied. (R_3) in the case that N contains two elements is satisfied vacuously. For suppose $r(N + e_1) = r(N + e_2) = r(N) = 2$. Then $N + e_1$ and $N + e_2$ are both in (16.1); but any two of these sets have but a single element in common.

[14] After the author had noted that M' satisfies (C^*) and corresponds to no linear graph, and had discovered a matroid with nine elements corresponding to no matrix, Saunders MacLane found that M' corresponds to no matrix, and is a well known example of a finite projective geometry (see O. Veblen and J. W. Young, *Projective* Geometry, pp. 3-5).

If there exists a matrix $\boldsymbol{M}'$, corresponding to M', then let $\boldsymbol{M}$ be its circuit matrix. 123 is a base in M', and hence

$$(16.2)\qquad 124, \quad 135, \quad 236, \quad 1237$$

form a fundamental set of circuits in M'. Let R_1, R_2, R_3, R_4 be the corresponding rows of $\boldsymbol{M}$. By multiplying in succession row 1, column 2, rows 2, 3, 4, and columns 4, 5, 6, 7 by suitable constants $\neq 0$, we bring $\boldsymbol{M}$ into the following form:

$$(16.3)\qquad \boldsymbol{M} = \left\|\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & a & 0 & 1 & 0 & 0 \\ 0 & 1 & b & 0 & 0 & 1 & 0 \\ 1 & c & d & 0 & 0 & 0 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right\|;$$

a, b, c and d are $\neq 0$. We now apply Theorem 32 with

$$(i_1, \cdots, i_s;\ j_1, \cdots, j_s) = (1, 4;\ 1, 2), \quad (2, 4;\ 1, 3), \quad (3, 4;\ 2, 3),$$

i. e. using the circuits 347, 257, 167. This gives

$$\begin{vmatrix} 1 & 1 \\ 1 & c \end{vmatrix} = \begin{vmatrix} 1 & a \\ 1 & d \end{vmatrix} = \begin{vmatrix} 1 & b \\ c & d \end{vmatrix} = 0,$$

and hence $c = 1$, $a = d = b$. Using the circuit 456, with sets $(1, 2, 3;\ 1, 2, 3)$ gives $2a = 0$, $a = 0$, a contradiction.

In regard to this example, see the end of the paper.

APPENDIX.

Matrices of Integers mod 2.

We wish to characterize those matroids M corresponding to matrices $\boldsymbol{M}$ of integers mod 2,[15] i. e. matrices whose elements are all 0 or 1, where rank etc. is defined mod 2. We shall consider linear combinations, *chains:*

$$(\text{A. }1)\qquad \alpha_1 e_1 + \cdots + \alpha_n e_n \qquad (\alpha\text{'s integers mod } 2)$$

in the elements of M. The α's may be taken as 0 or 1; (A. 1) may then be interpreted as the submatroid N whose elements have the coefficient 1. Conversely, any $N \subset M$ may be written as a chain. Submatroids are added

[15] See O. Veblen, "Analysis situs," 2nd ed., *American Mathematical Society Colloquium Publications*, Ch. I and Appendix 2.

(mod 2) by adding the corresponding chains (mod 2). For instance, $(e_1+e_2)+(e_2+e_3)\equiv e_1+e_3$ (mod 2).

Any sum (mod 2) of circuits in M we shall call a *cycle* in M. N is the *true sum* of $N_1,\cdots,N_s$ if these latter have no common elements and $N=N_1+\cdots+N_s$. We consider matroids which satisfy the following postulate:

(C*) *Each cycle is a true sum of circuits.*

Postulate (C_2) is a consequence of (C*). For the cycle P_1+P_2 is a submatroid containing e_2 but not e_1; The existence of P_3 now follows from (C*).

A simple example of a matroid not satisfying (C*) is given by the matroid M' at the end of § 9.

THEOREM 33. *A circuit is a minimal non-null cycle, and conversely.*

This is proved with the aid of Postulates (C_1) and (C*).

THEOREM 34. *Let $P_1,\cdots,P_q$ be a strict fundamental set of circuits in M with respect to $e_{n-q+1},\cdots,e_n$. Then there are exactly 2^q cycles in M, formed by taking all sums* (mod 2) *of $P_1,\cdots,P_q$.*

First, each sum $P_{i_1}+\cdots+P_{i_s}$ (mod 2) is a cycle, containing $e_{n-q+i_1},\cdots,e_{n-q+i_s}$ and elements (perhaps) from $B=e_1,\cdots,e_{n-q}$; obviously distinct sums give distinct cycles. Now let Q be any cycle in M; say Q contains $e_{n-q+k_1},\cdots,e_{n-q+k_r}$ and elements (perhaps) from B. Set $Q'=P_{k_1}+\cdots+P_{k_r}$; then $Q+Q'$ is a cycle containing elements from B alone. But B is a base (see the proof of Theorem 10), and hence contains no circuits. Consequently $Q+Q'$ is the null cycle, and $Q=Q'$.

THEOREM 35. *As soon as the circuits of a strict fundamental set are known, all the circuits may be determined.*

This is a consequence of the last two theorems. It is to be contrasted with the final remark of § 9.

Remark. The word "strict" may be omitted in the last two theorems.

THEOREM 36. *Let $e_1,\cdots,e_n$ be a set of elements, and let $P_1,\cdots,P_q$ be any subsets such that P_i contains e_{n-q+i} and possibly elements from $e_1,\cdots,e_{n-q}$ alone. Then there is a unique matroid M satisfying* (C*), *with $P_1,\cdots,P_q$ as a strict fundamental set of circuits.*

We form the 2^q cycles of Theorem 34. Those cycles which contain no other non-null cycle as a proper subset we call circuits; in particular, $P_1, \cdots, P_q$ are circuits. To prove (C*), let Q be a non-null cycle. If it is not a circuit, it contains a circuit P as a proper subset. Q and P are sums (mod 2) from $P_1, \cdots, P_q$, hence the same is true of $Q - P$, and $Q - P$ is one of the 2^q cycles. If it is not a circuit, we again extract a circuit, etc.

This theorem furnishes a simple method of constructing all matroids satisfying (C*).

We turn now to the study of matrices of integers (mod 2)

$$\boldsymbol{M} = \begin{Vmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdot\ \cdot & \cdot \\ a_{m1} & \cdots & a_{mn} \end{Vmatrix} \qquad \text{(each } a_{ij} = 0 \text{ or } 1\text{)}.$$

Any linear combination (mod 2) of the columns

$$\text{(A. 2)} \qquad \alpha_1 C_1 + \cdots + \alpha_n C_n \qquad (\alpha\text{'s integers mod } 2)$$

is a set of numbers $(\Sigma \alpha_i a_{1i}, \cdots, \Sigma \alpha_i a_{mi})$, which we call a *chain* (mod 2) in $\boldsymbol{M}$. As before, we may take each coefficient as 0 or 1, and we may consider any chain merely as a submatrix of $\boldsymbol{M}$. The chain is a *cycle* if each of the corresponding numbers is $\equiv 0$ (mod 2). The columns $C_{i_1}, \cdots, C_{i_p}$ are *independent* (mod 2) if there exists no set of integers $\alpha_1, \cdots, \alpha_n$ not all $\equiv 0$ (mod 2), with $\alpha_i = 0$ $(i \neq i_1, \cdots, i_p)$, such that $\Sigma \alpha_i C_i$ is a cycle, i. e. if no non-null subset of $C_{i_1}, \cdots, C_{i_p}$ is a cycle. Using this definition, the terms base, circuit, rank, nullity etc. (mod 2) can be defined as in Part I.

Let M be a set of elements $e_1, \cdots, e_n$ corresponding to $C_1, \cdots, C_n$ in $\boldsymbol{M}$, and let $e_{i_1} + \cdots + e_{i_p}$ be a circuit in M if and only if $C_{i_1}, \cdots, C_{i_p}$ is a circuit in $\boldsymbol{M}$. We shall show that *M is a matroid satisfying* (C*) *and the definitions of cycle in M and $\boldsymbol{M}$ agree.*

We show first that each circuit is a cycle in $\boldsymbol{M}$. If $C_{i_1}, \cdots, C_{i_p}$ is a circuit, then these columns are dependent; hence $\Sigma \alpha_i C_i$ is a cycle, with $\alpha_i = 0$ $(i \neq i_1, \cdots, i_p)$. Moreover $\alpha_i = 1$ $(i = i_1, \cdots, i_p)$, for otherwise a proper subset of $C_{i_1}, \cdots, C_{i_p}$ would be dependent. Hence $C_{i_1} + \cdots + C_{i_p}$ is a cycle. Next, any sum (mod 2) of circuits is a cycle, evidently. Next we prove (C*). Suppose $Q = C_{i_1} + \cdots + C_{i_p}$ is a cycle. Let $(k_1, \cdots, k_q)$ be a minimal subset of $(i_1, \cdots, i_p)$ such that $P = C_{k_1} + \cdots + C_{k_q}$ is a cycle; then P is a circuit. $Q - P$ is a cycle; from it we extract a circuit, just as above, etc. It follows from (C*) that the definitions of cycle in M and $\boldsymbol{M}$ agree. Theorems 33, 34 and 35 now apply to $\boldsymbol{M}$ also.

We are now ready to prove the final theorem:

THEOREM 37. *Let M be any matroid satisfying* (C*). *Suppose $\rho(M) = n$, and $e_1 + \cdots + e_{n-q}$ is a base. Then if $\boldsymbol{M}_1$ is any matrix of integers* (*mod* 2) *with $n - q$ columns which are independent* (*mod* 2), *columns $C_{n-q+1}, \cdots, C_n$ can be adjoined in a unique manner to $\boldsymbol{M}_1$, forming a matrix $\boldsymbol{M}$ of which the corresponding matroid is M.*

Let $P_1, \cdots, P_q$ be a strict fundamental set of circuits in M with respect to $e_{n-q+1}, \cdots, e_n$ (Theorem 9). Say $P_1 = e_{i_1} + \cdots + e_{i_p} + e_{n-q+1}$. Set $C_{n-q+1} \equiv C_{i_1} + \cdots + C_{i_p}$ (mod 2); this determines C_{n-q+1} as a column of 0's and 1's so that $P'_1 = C_{i_1} + \cdots + C_{i_p} + C_{n-q+1}$ is a circuit. (P'_1 is a cycle; (C*) shows that it is a single circuit, as $C_1 + \cdots + C_{n-q}$ contains no circuit.) C_{n-q+1} evidently must be chosen in this manner. We choose the remaining columns of $\boldsymbol{M}$ similarly. Let M' be the matroid corresponding to $\boldsymbol{M}$. Then $P'_1, \cdots, P'_q$ is a strict set of circuits in M'. These same sets form a strict set in M; hence, by Theorem 35, the circuits in M' correspond to those in M. Consequently $M' = M$, completing the proof.

We end by noting that the matroid M' of § 16 satisfies Postulate (C*) but corresponds to no linear graph. For letting 123 be a base and (16.2) a fundamental set of circuits and determining the matroid as in Theorem 36, we come out with exactly M'. A corresponding matrix of integers mod 2 is constructed from (16.3) with $a = b = c = d = 1$; we interchange rows and columns in the left-hand portion, leave out the last row and column of the right-hand portion, and interchange these two parts. (The relation $2a = 0$ is of course true mod 2.)

On the other hand, it is easily seen that if the element 7 is left out, there is a corresponding graph, which must be of the following sort: It has four vertices a, b, c, d, and the arcs corresponding to the elements $1, \cdots, 6$ are

$$ab, \quad ac, \quad ad, \quad bc, \quad bd, \quad cd.$$

There is no way of adding the required seventh arc.

The problem of characterizing linear graphs from this point of view is the same as that of characterizing matroids which correspond to matrices (mod 2) with exactly two ones in each column.

HARVARD UNIVERSITY.